FORCEnet
engineering conference

November 15 - 17, 2005: Town & Country Convention Center - San Diego, CA

PMW 160 Information Assurance 101

Dr. Gus Lott

Principal Engineer,

YARCOM

17 November, 2005

Approved for public release; distribution is unlimited

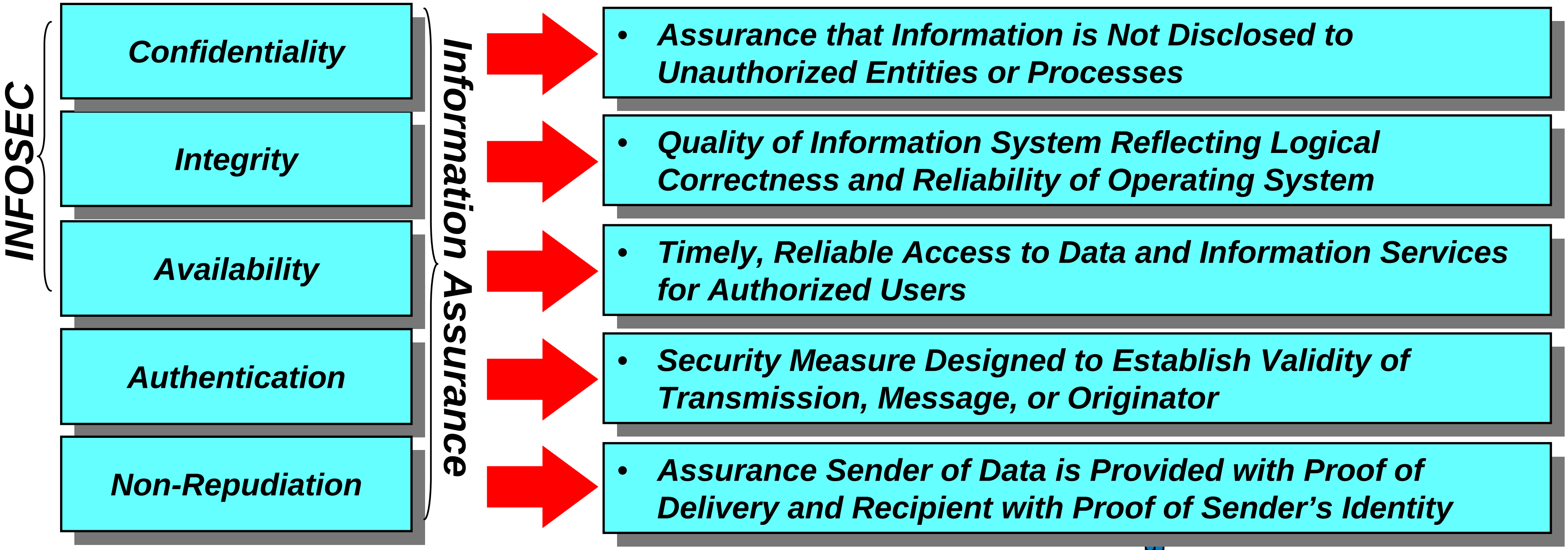
Sponsored by SPAWAR
SPAWARSYSCOM
FORCEnet Chief Engineer

Objectives

- What is Information Assurance?
- Why should you care about IA?
- What are some of the core concepts of IA?
- Where can you go for help.

What is Information Assurance (IA)?

"Measures that Protect and Defend Information and Information Systems by Ensuring Their Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation. This Includes Providing for Restoration of Information Systems by Incorporating Protection, Detection, and Reaction Capabilities."



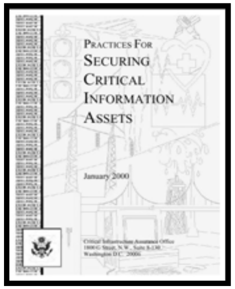
Confidentiality	• *Assurance that Information is Not Disclosed to Unauthorized Entities or Processes*
Integrity	• *Quality of Information System Reflecting Logical Correctness and Reliability of Operating System*
Availability	• *Timely, Reliable Access to Data and Information Services for Authorized Users*
Authentication	• *Security Measure Designed to Establish Validity of Transmission, Message, or Originator*
Non-Repudiation	• *Assurance Sender of Data is Provided with Proof of Delivery and Recipient with Proof of Sender's Identity*

DoD Directive 8500.1
24 October 2002

Why Should You Care About Information Assurance (IA)?

Presidential Decision Directive 63 (May 1998)

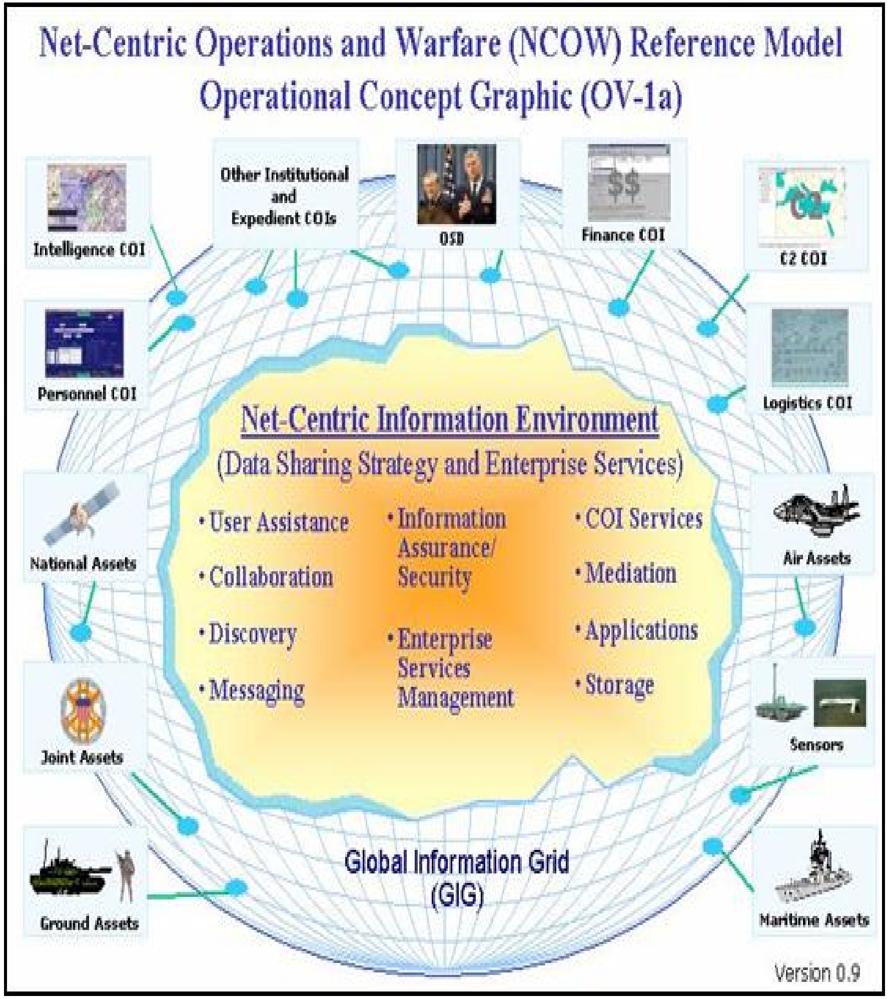
"… a national effort to ensure the security of the increasingly vulnerable and interconnected infrastructure of the United States, especially the cyber-based infrastructure."



Practices For Securing Critical Information Assets

January 2000

Critical Infrastructure Assurance Office
1300 G Street, N.W., Suite 8-130
Washington D.C. 20006

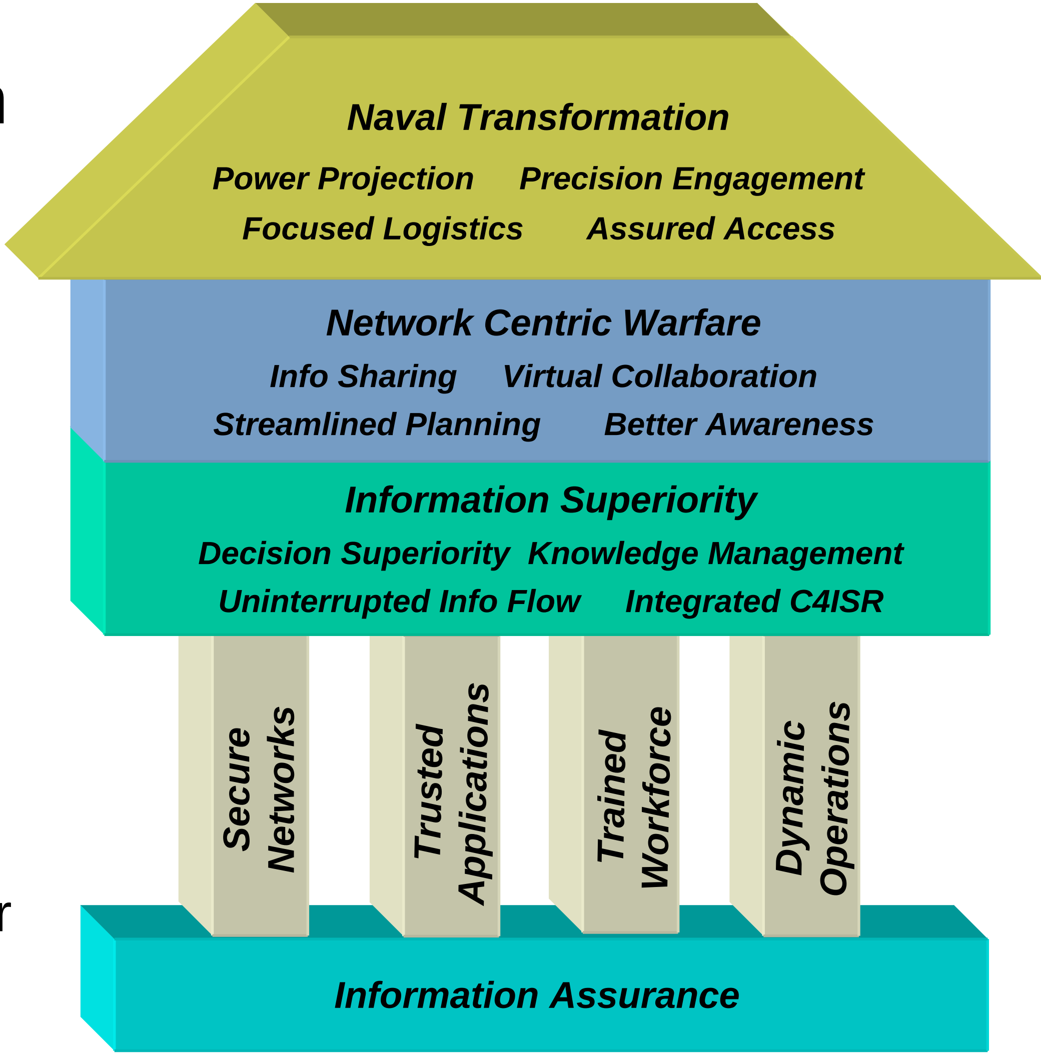


Net-Centric Operations and Warfare (NCOW) Reference Model
Operational Concept Graphic (OV-1a)
Intelligence COI
Other Institutional and Expedient COIs
OSD
Finance COI
C2 COI
Personnel COI
Logistics COI
Net-Centric Information Environment
(Data Sharing Strategy and Enterprise Services)
• User Assistance
• Collaboration
• Discovery
• Messaging
• Information Assurance/ Security
• Enterprise Services Management
• COI Services
• Mediation
• Applications
• Storage
National Assets
Air Assets
Joint Assets
Sensors
Ground Assets
Maritime Assets
Global Information Grid (GIG)
Version 0.9

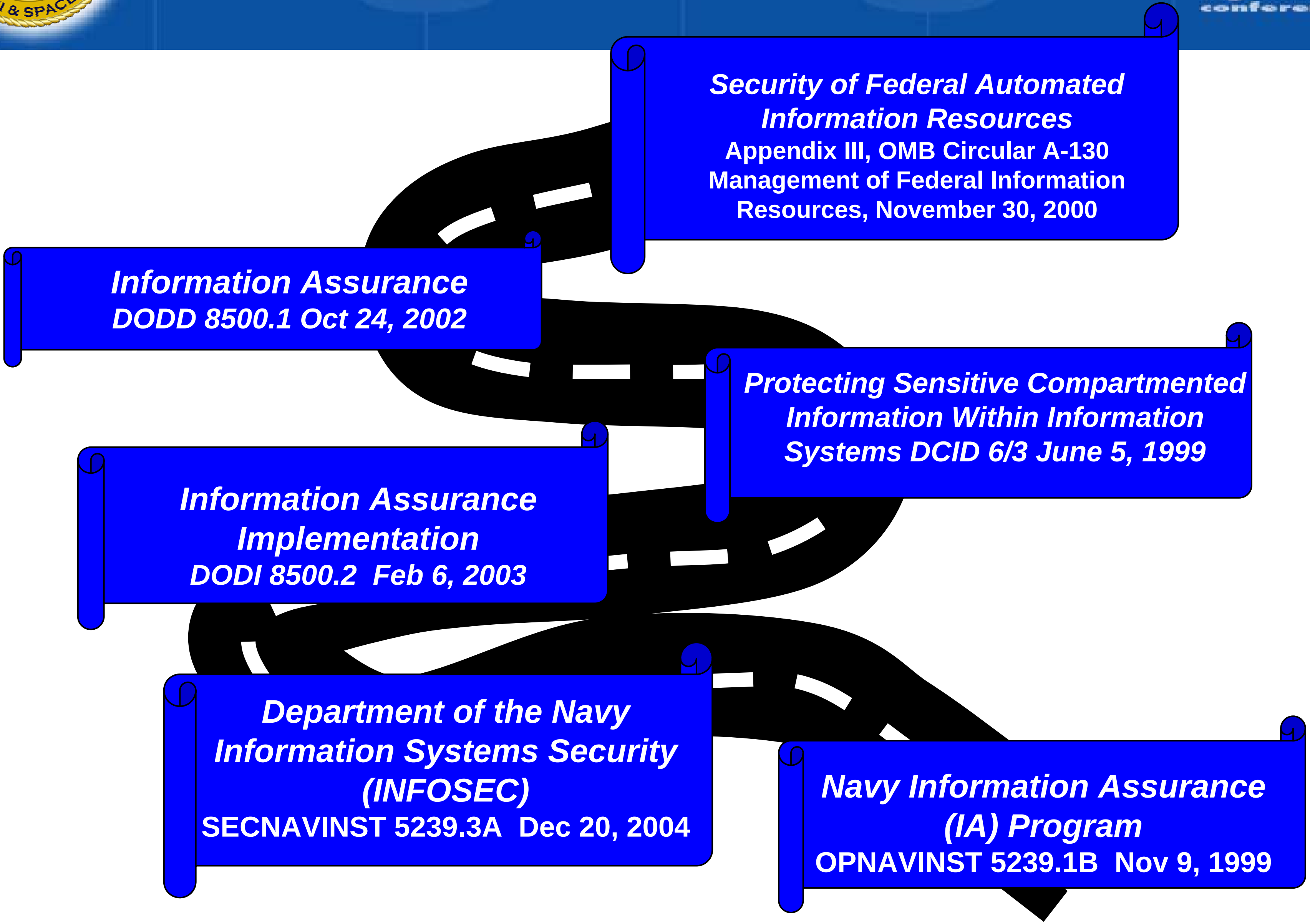
In a net-centric world, a risk taken by one is a risk shared by all

IA is an Enabler for all Information Systems

- We Count on Information Superiority to Improve Combat Effectiveness
  - Full Spectrum Dominance
  - Network Centric Warfare
- IA Enables Information Superiority in a Network-Centric Paradigm
  - Global Secure, Interoperable Network
  - State-of-the Art Protection for Information Infrastructure



USN Compliance Roadmap



Security of Federal Automated Information Resources
Appendix III, OMB Circular A-130 Management of Federal Information Resources, November 30, 2000

Information Assurance
DODD 8500.1 Oct 24, 2002

Protecting Sensitive Compartmented Information Within Information Systems DCID 6/3 June 5, 1999

Information Assurance Implementation
DODI 8500.2 Feb 6, 2003

Department of the Navy Information Systems Security (INFOSEC)
SECNAVINST 5239.3A Dec 20, 2004

Navy Information Assurance (IA) Program
OPNAVINST 5239.1B Nov 9, 1999

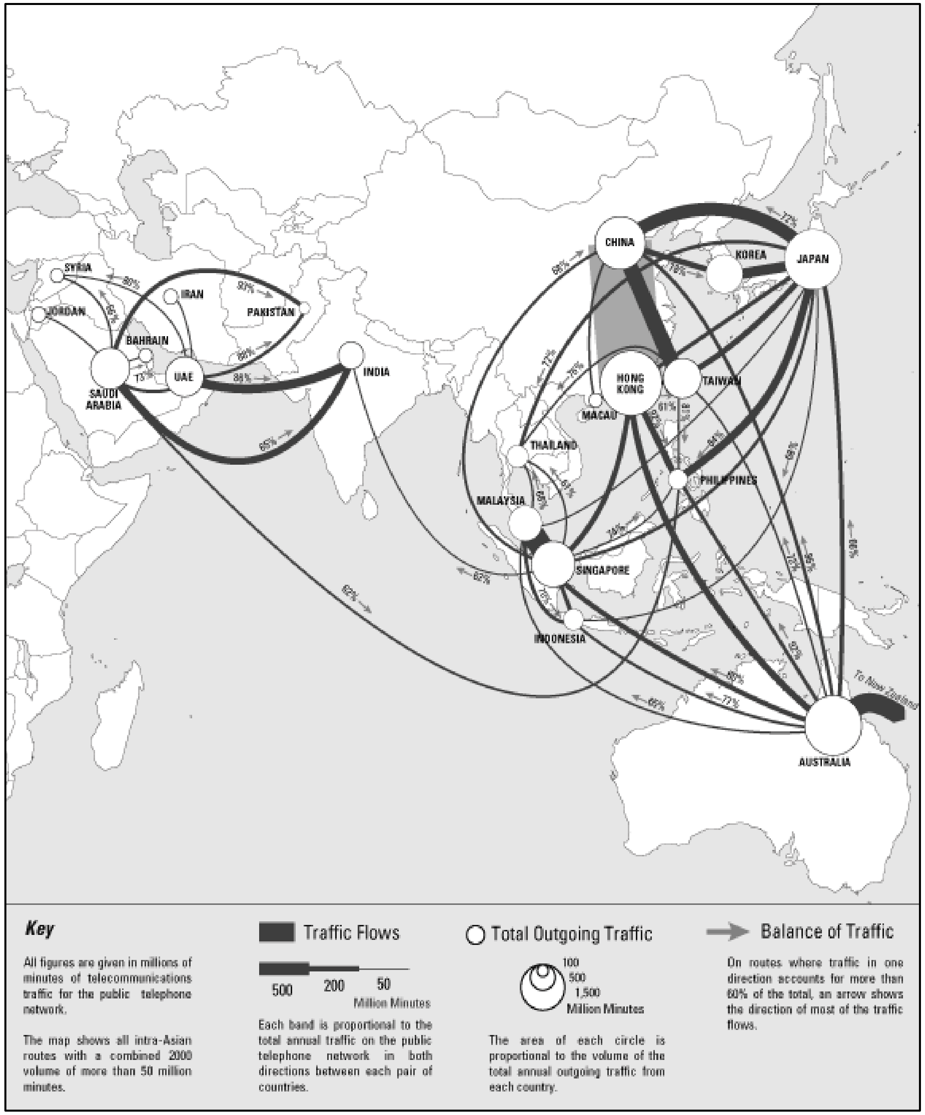
Support to FORCEnet

- Compliance with interoperability statutes and the <u>Defense Standardization Program</u> (10 USC 2451, 10 USC 2452, & DODI 4120.24)
- Lead development of the Fn architecture Technical View – IA standards sections – Mandated standards and emerging standards
- Also supporting the Maritime Cryptologic Architecture TV 3.1 development

Mobile Code example

- **IA control DCMC-1, DODI 8500.2**
- **FORCENET development will minimize the use of category 1 mobile code technologies, based upon risk management, capability required, and economic analysis. Where necessary, all category 1 mobile code will be digitally signed using DOD PKI and using industry standard techniques such as Microsoft Authenticode™.**
- **FORCENET use of Java category 2 mobile code will include the COTS security model for (1) Sun Java™ 2.0 (Security Code Guidelines February 2000) or (2) Microsoft J++ (Trust-Based Security for Java April 2000). All FORCENET Java applets will be signed using Javakey, Signkey, or Authenticode technologies.**
- **FORCENET scripting languages will comply with EMCA-262/ISO-16262 standard scripting language or Netscape Javascript version 1.5.**
- **FORCENET web scripting services will comply with World Wide Web Consortium standard XHTML™ 1.0, "The Extensible Hypertext Markup Language," which is a reformulation of HTML 4 in XML 1.0, January 2000.**

Who’s calling or typing?



Key

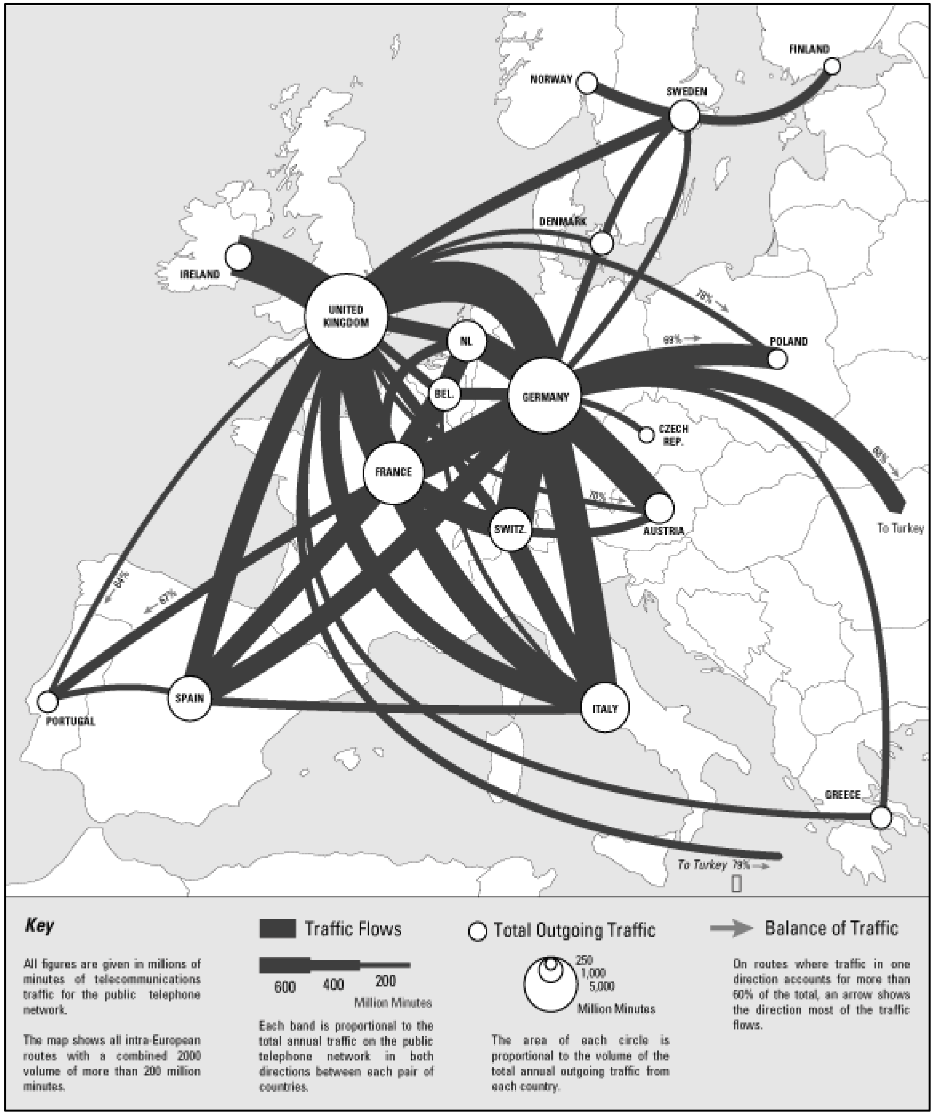
All figures are given in millions of minutes of telecommunications traffic for the public telephone network.

The map shows all intra-Asian routes with a combined 2000 volume of more than 50 million minutes.

Each band is proportional to the total annual traffic on the public telephone network in both directions between each pair of countries.

The area of each circle is proportional to the volume of the total annual outgoing traffic from each country.

On routes where traffic in one direction accounts for more than 60% of the total, an arrow shows the direction of most of the traffic flows.



Key

All figures are given in millions of minutes of telecommunications traffic for the public telephone network.

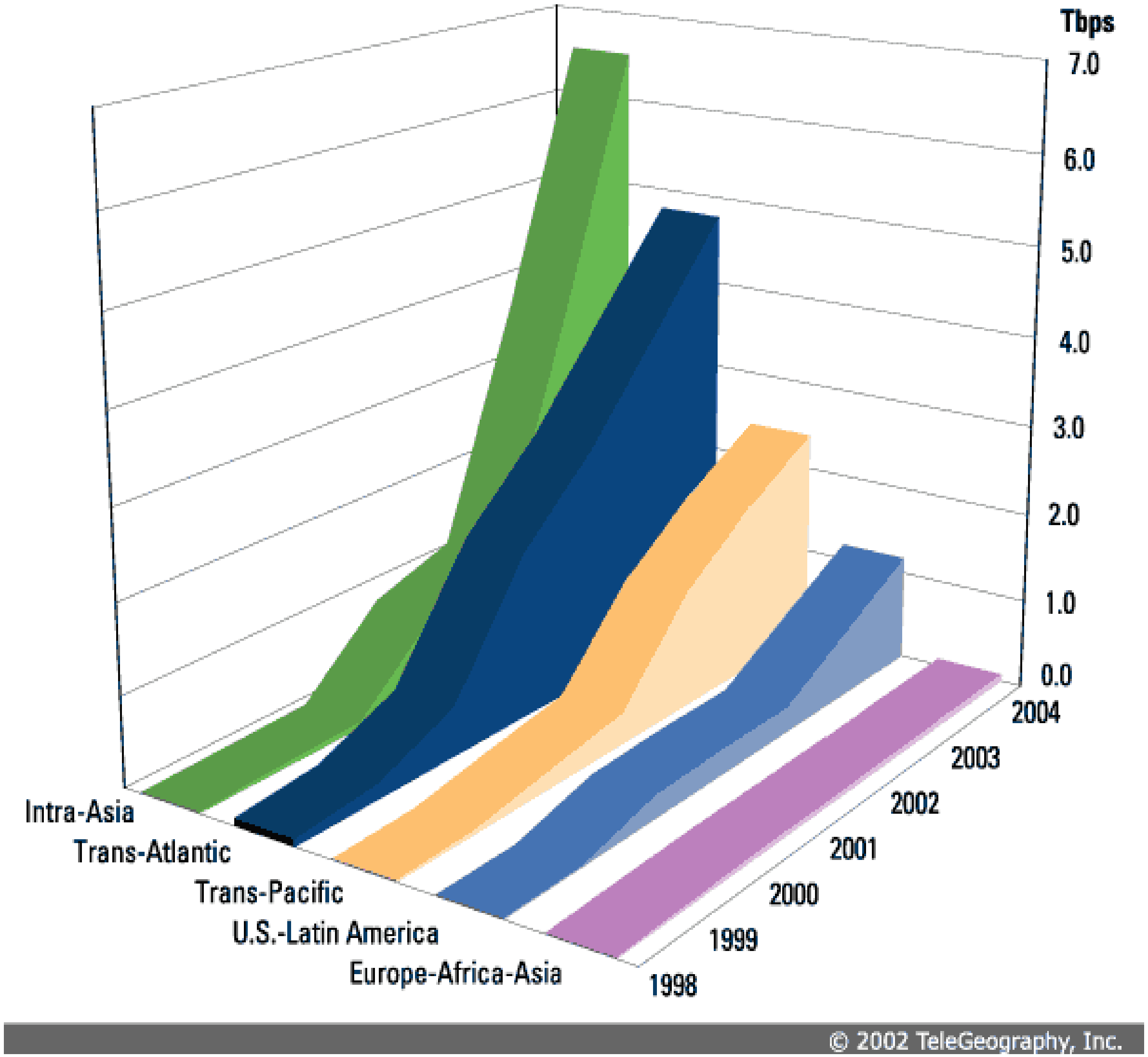
The map shows all intra-European routes with a combined 2000 volume of more than 200 million minutes.

Each band is proportional to the total annual traffic on the public telephone network in both directions between each pair of countries.

The area of each circle is proportional to the volume of the total annual outgoing traffic from each country.

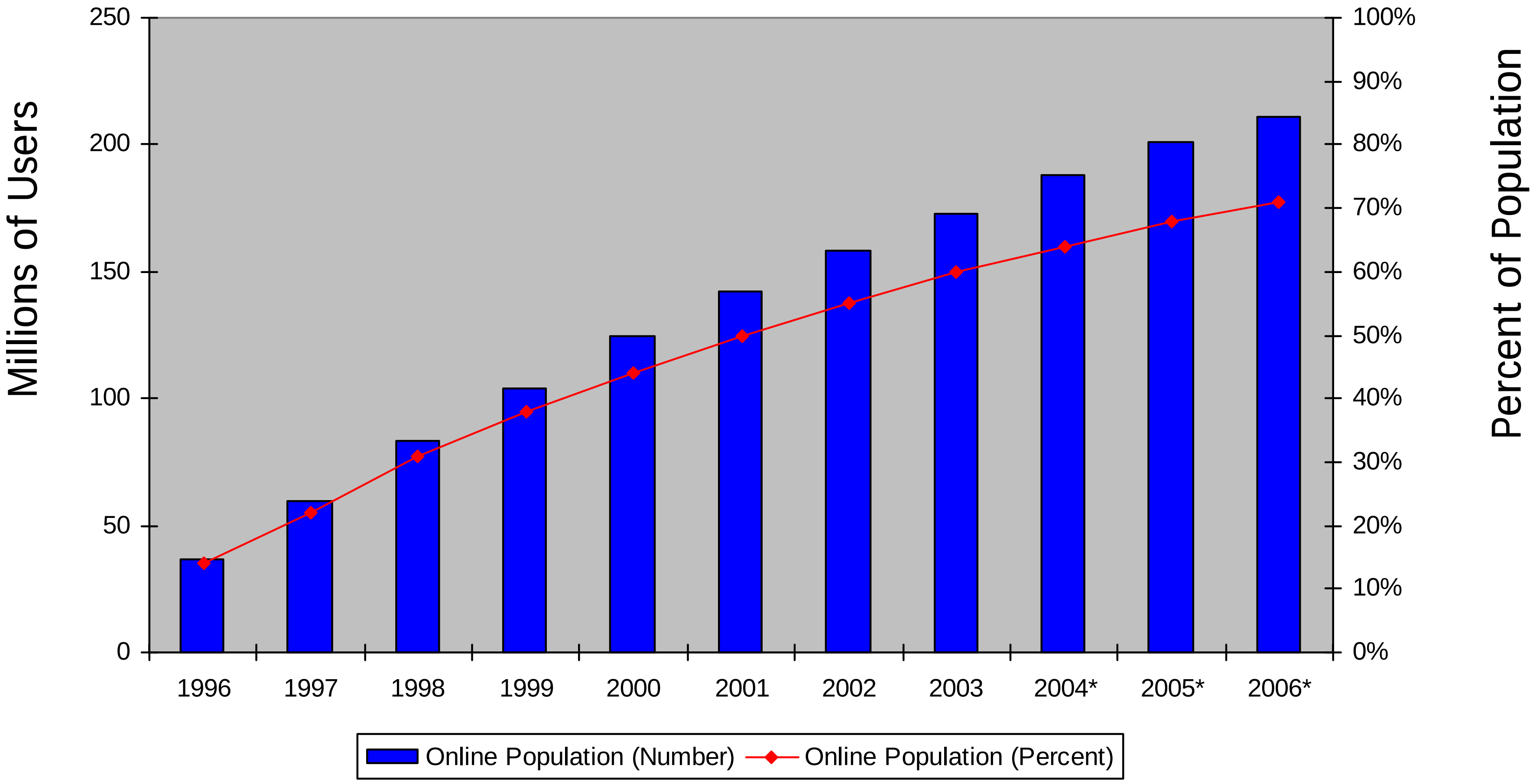
On routes where traffic in one direction accounts for more than 60% of the total, an arrow shows the direction most of the traffic flows.

Growth of Fiber Connectivity



© 2002 TeleGeography, Inc.

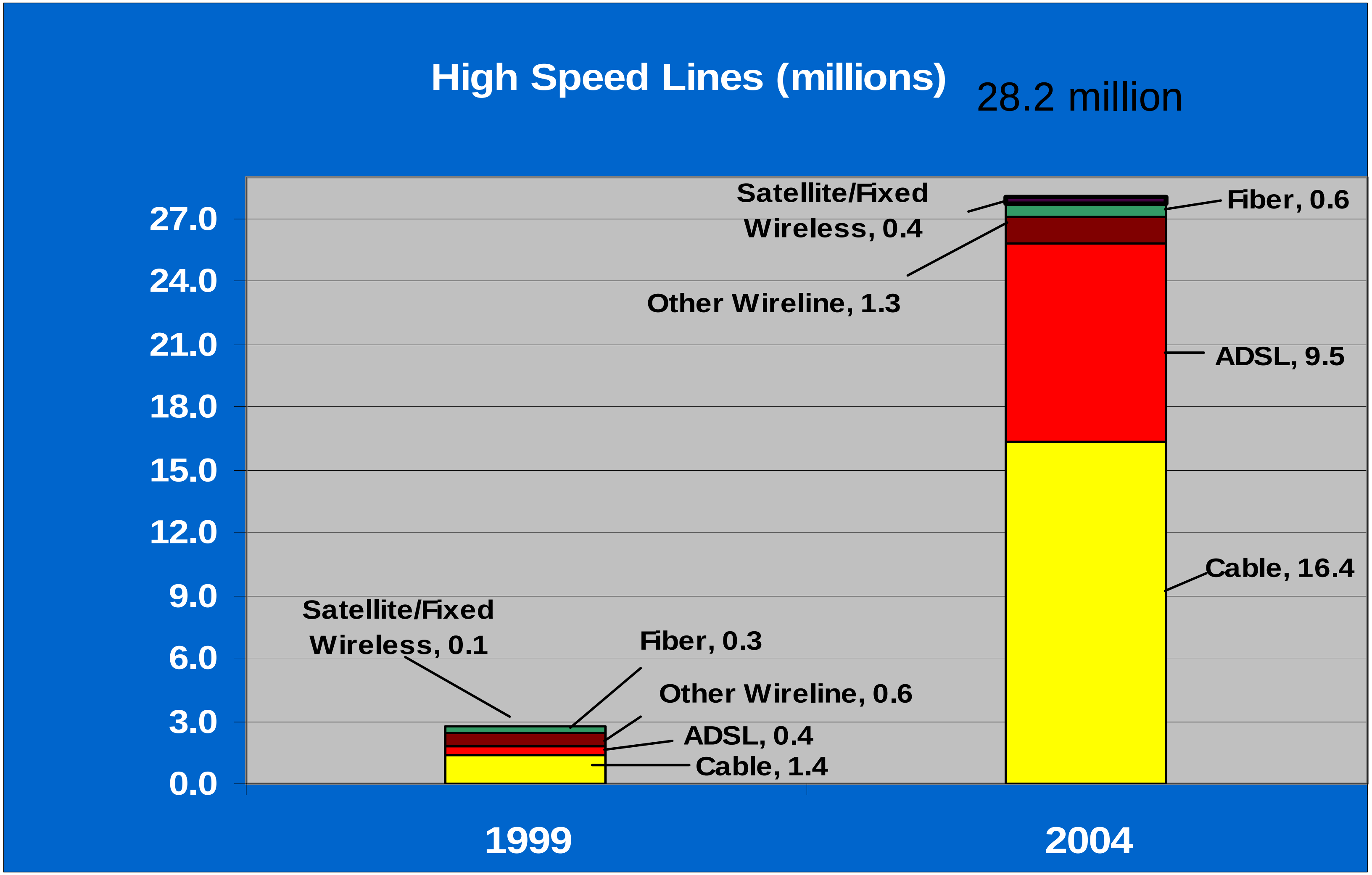
Internet Growth
US Households Online



Source: The Digital Economy Fact Book, Fifth Edition 2003

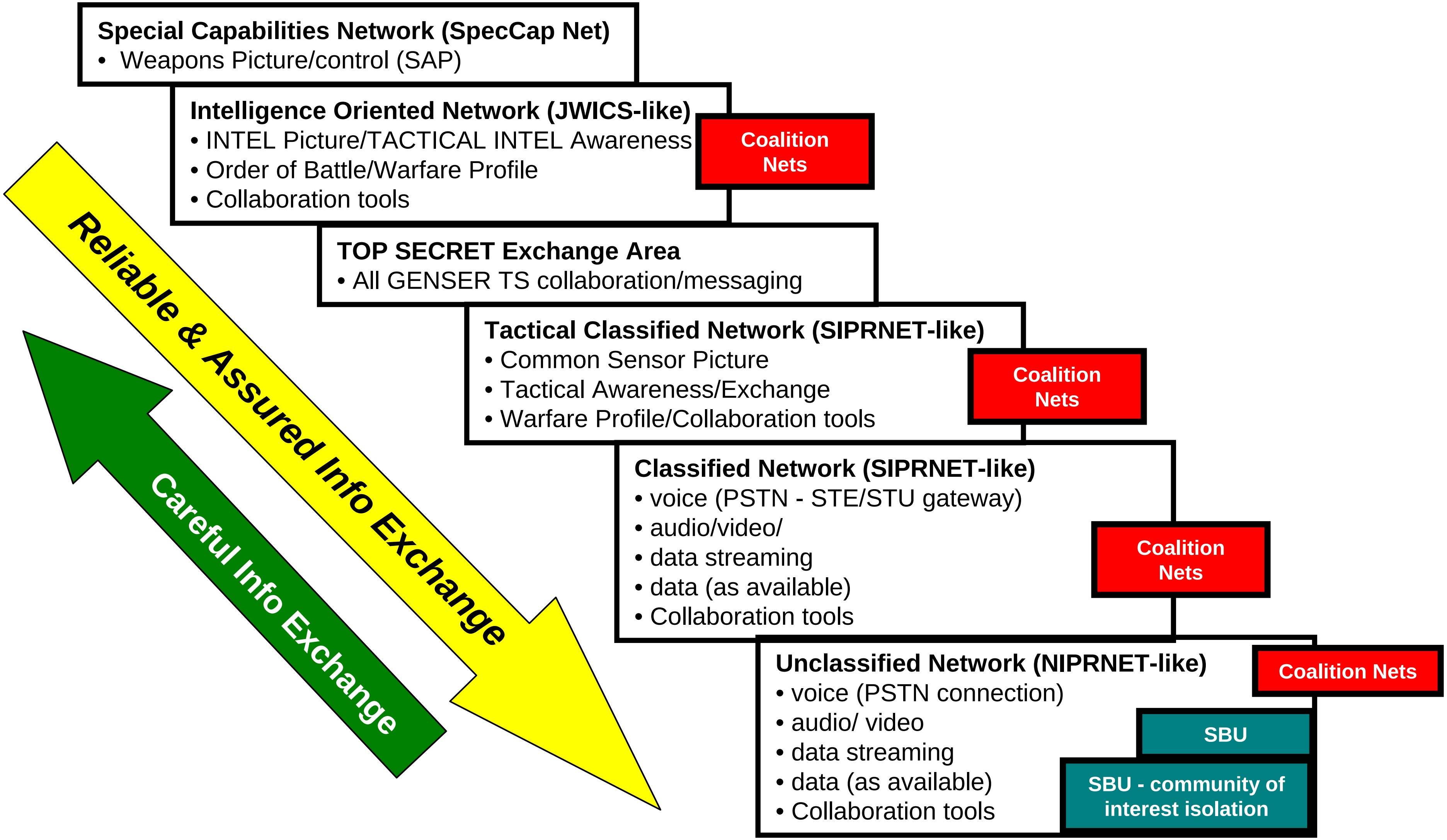
High Speed Line Growth 1999-2004

FORCEnet engineering conference



Source: FCC's High Speed Services for Internet Access Report, 6/04

Information Communities



Special Capabilities Network (SpecCap Net)
- Weapons Picture/control (SAP)

Intelligence Oriented Network (JWICS-like)
- INTEL Picture/TACTICAL INTEL Awareness
- Order of Battle/Warfare Profile
- Collaboration tools

Coalition Nets

TOP SECRET Exchange Area
- All GENSER TS collaboration/messaging

Tactical Classified Network (SIPRNET-like)
- Common Sensor Picture
- Tactical Awareness/Exchange
- Warfare Profile/Collaboration tools

Coalition Nets

Classified Network (SIPRNET-like)
- voice (PSTN - STE/STU gateway)
- audio/video/
- data streaming
- data (as available)
- Collaboration tools

Coalition Nets

Unclassified Network (NIPRNET-like)
- voice (PSTN connection)
- audio/ video
- data streaming
- data (as available)
- Collaboration tools

Coalition Nets

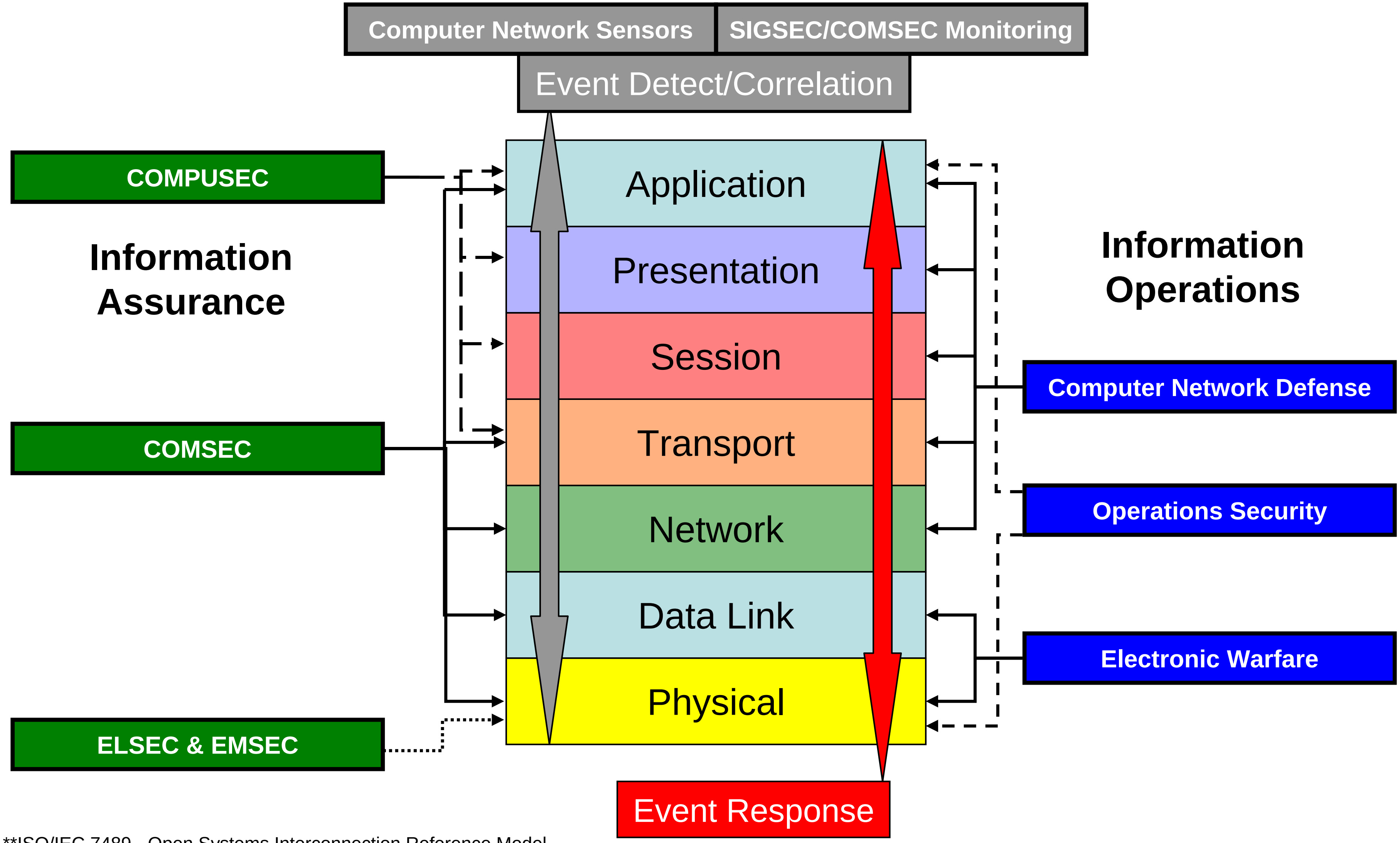
SBU

SBU - community of interest isolation

National Security Info

- Title 40 USC Chapter 25 Sec. 1452
  - (a) “In this part, the term "national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which -
    - **(1) involves intelligence activities;**
    - **(2) involves cryptologic activities related to national security;**
    - **(3) involves command and control of military forces;**
    - **(4) involves equipment that is an integral part of a weapon or weapons system; or**
    - **(5) subject to subsection (b) of this section, is critical to the direct fulfillment of military or intelligence missions.**
  - (b) Limitation Subsection (a)(5) of this section does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).”
- May be Classified or Unclassified

IA Across the Stack



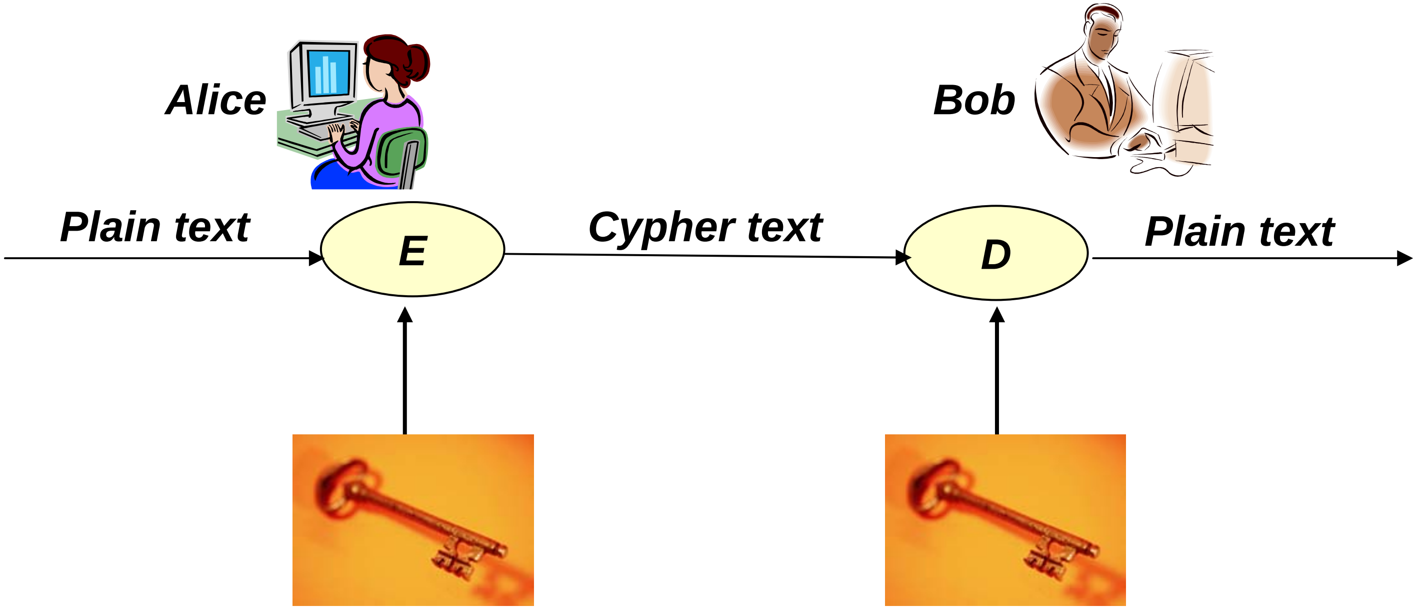
**ISO/IEC 7489 - Open Systems Interconnection Reference Model

Crypto Security

- Provisioning of technically sound cryptographic systems and their proper use.
- Cryptography is derived from the Greek words: kryptós, "hidden", and gráphein, "to write" - or "hidden writing“.
- Denies access to the information by an unauthorized recipient for an estimated period of time
- Includes an entire system
  - Algorithm
  - Appliances
  - Key Management Infrastructure
  - Policies and Procedures

Symmetric System

- Encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret.

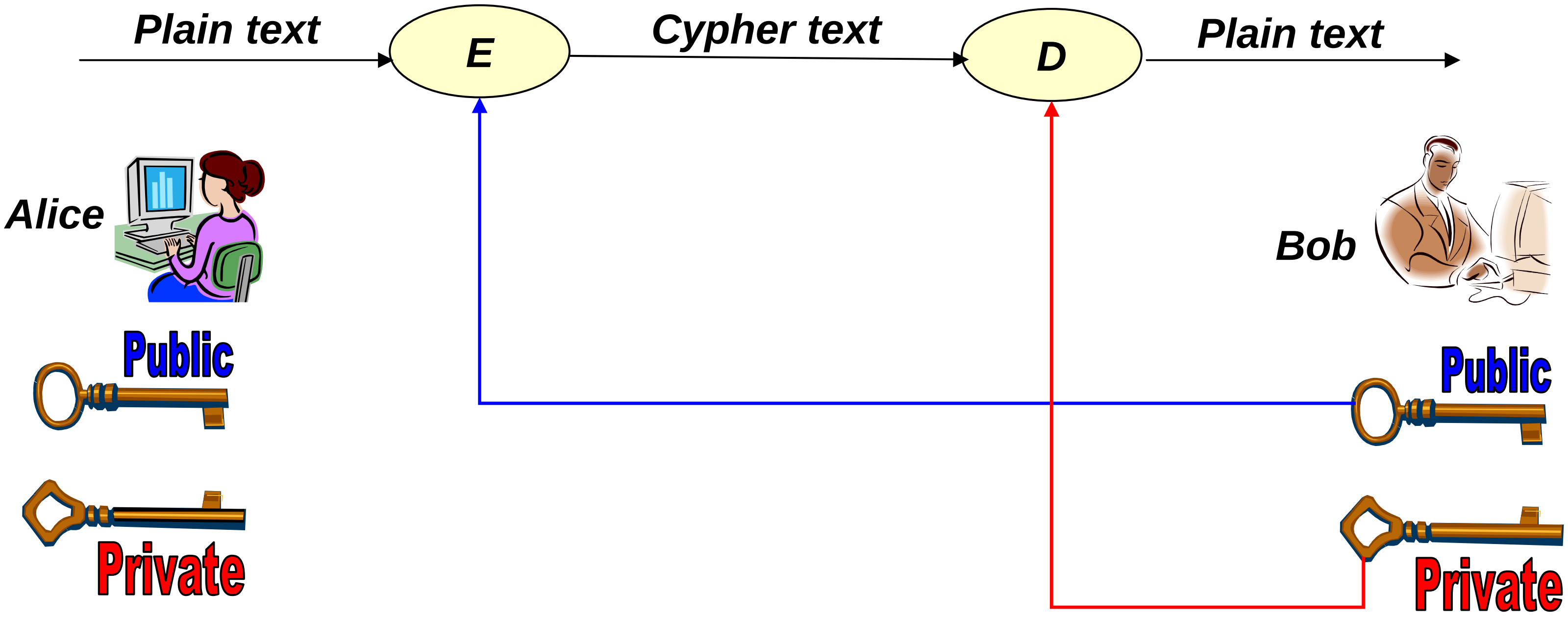


Key known to both

Kept SECRET from all others

Asymmetric System

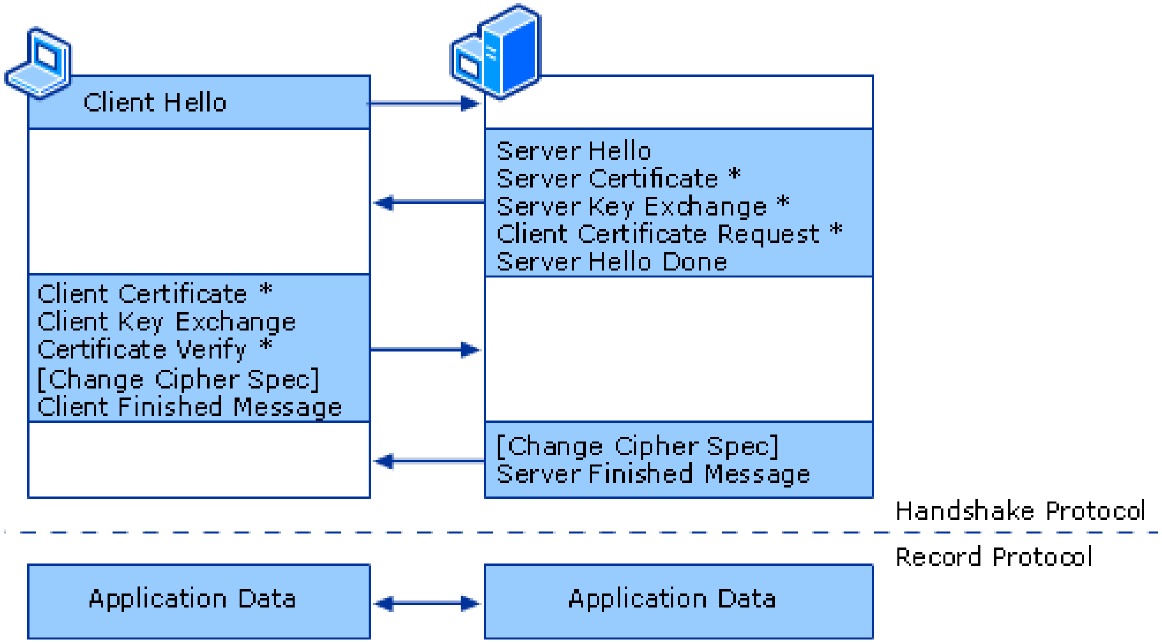
- Two key parts – public & private
- Encrypt with public key and decrypt with private key



TLS/SSL

Network Ports Used by TLS/SSL
Port Assignments for Common Applications over TLS/SSL

Service Name	TCP
smtp	25
https	443
nntps	563
ldaps	636
ftps-data	989
ftps	990
telnets	992
imaps	993
pop3s	995
ms-sql-s	1433
mfst-gc-ssl	3269
tftps	3713



Client Hello

Server Hello
Server Certificate *
Server Key Exchange *
Client Certificate Request *
Server Hello Done

Client Certificate *
Client Key Exchange
Certificate Verify *
[Change Cipher Spec]
Client Finished Message

[Change Cipher Spec]
Server Finished Message

Handshake Protocol

Record Protocol

Application Data

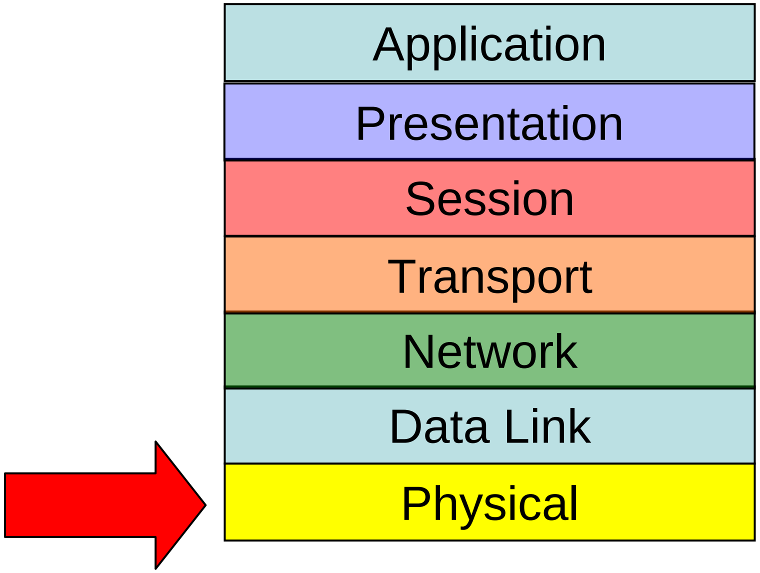
Application Data

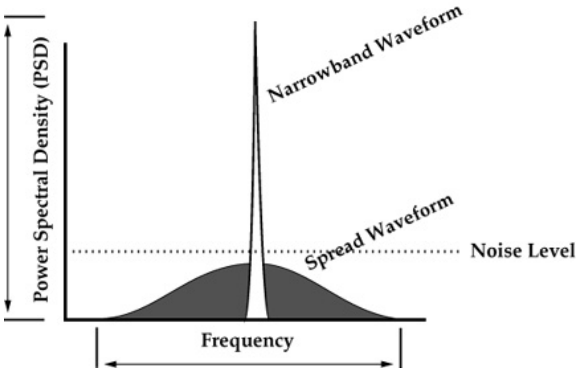
* Optional or situation-dependent messages

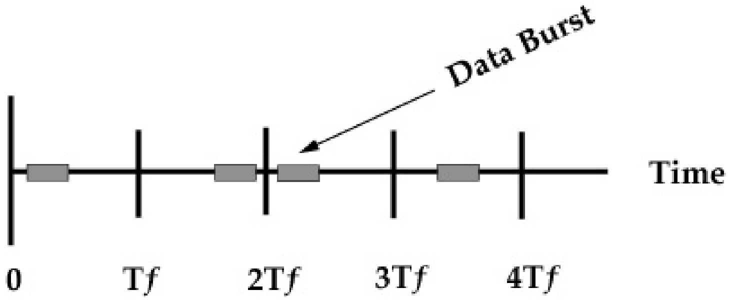
[Change Cipher Spec] is not a TLS handshake message but is an independent, TLS Protocol content type that helps the parties avoid a pipeline stall.

TRANSEC

- Five basic methods
  - Direct Sequence
  - Frequency Hopping
  - Time Hopping
  - Pulsed FM (Chirp)
  - Short-Duration (Burst)


Application
Presentation
Session
Transport
Network
Data Link
Physical





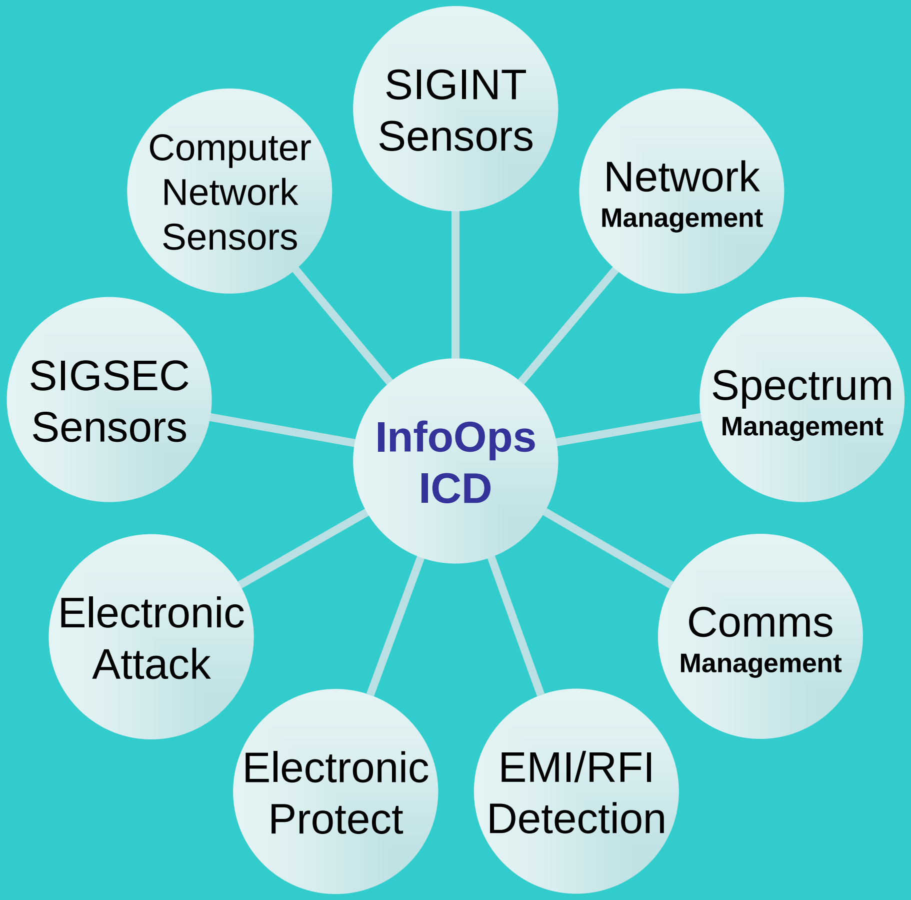
OPSEC

- What is OPSEC (DODD 5200.5) ?
  - A process of identifying critical information and subsequently analyzing friendly actions attendant to defense acquisition, defense activities, military operations, and other activities to:
    - Identify those **actions** that may be **observed by adversary** intelligence systems.
    - Determine what indicators hostile intelligence systems may obtain that could be interpreted or pieced together to **derive critical information in time to be useful** to adversaries.
    - Select and execute **measures that eliminate or reduce to an acceptable level the vulnerabilities** of friendly actions to adversary exploitation.

Physical Security

- Availability
- Most Effective Denial of Service Attack = Backhoe
- Threats – to hardware and software
  - Power loss
  - Fire or water damage
  - Disaster
  - Contamination
  - Theft
  - Hostile Attack
- Think restoration and recovery
- Sensors to detect problems before they become severe

Availability Through Coordination



InfoOps ICD

SIGINT Sensors

Network Management

Spectrum Management

Comms Management

EMI/RFI Detection

Electronic Protect

Electronic Attack

SIGSEC Sensors

Computer Network Sensors

Vulnerability and Threat Definitions

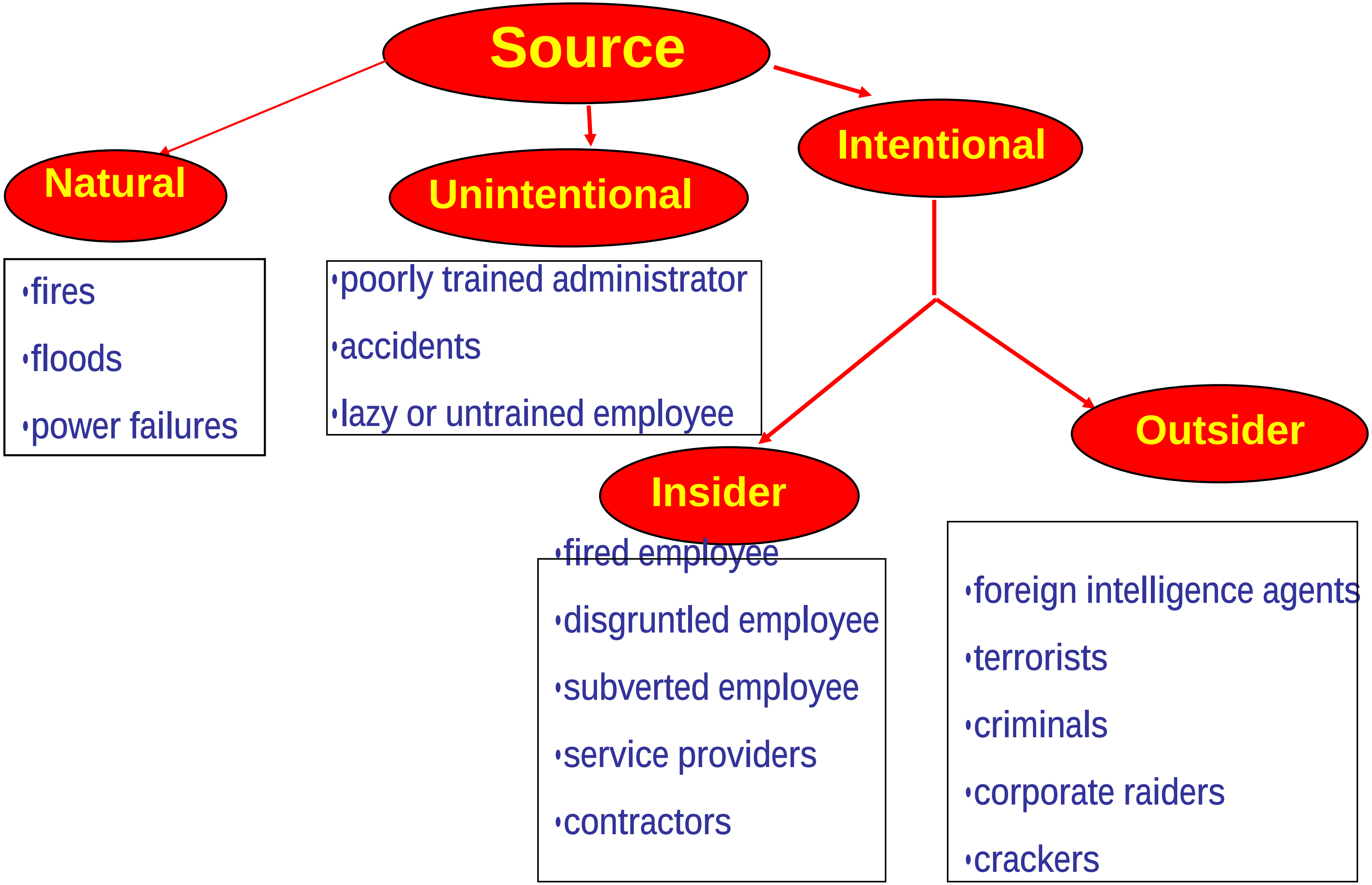
Vulnerability

Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited.

Threat

Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event that will cause harm or has the potential to cause harm to, information or an information system.

Threat Vectors



Source

Natural

- fires
- floods
- power failures

Unintentional

- poorly trained administrator
- accidents
- lazy or untrained employee

Intentional

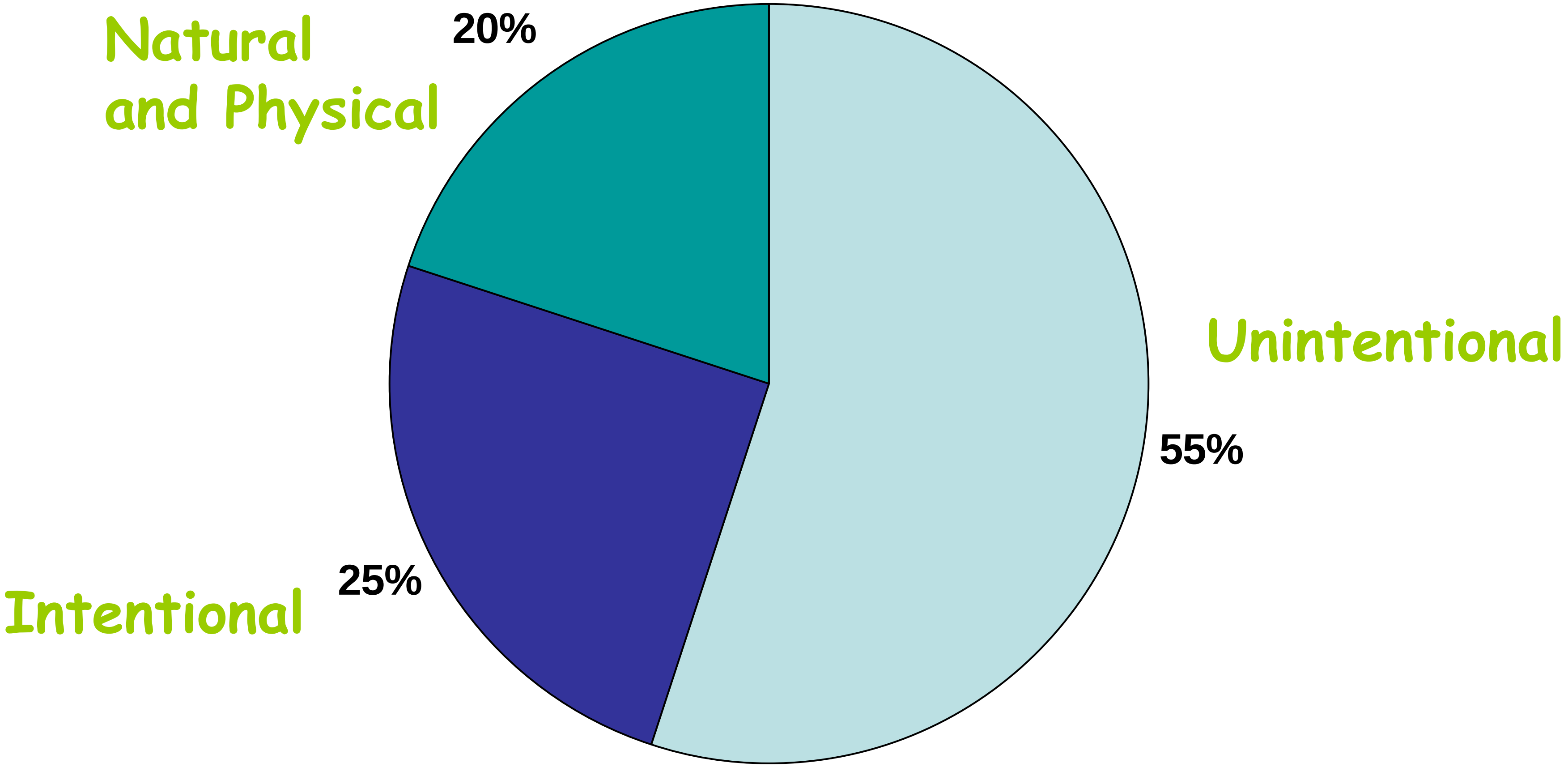
Insider

- fired employee
- disgruntled employee
- subverted employee
- service providers
- contractors

Outsider

- foreign intelligence agents
- terrorists
- criminals
- corporate raiders
- crackers

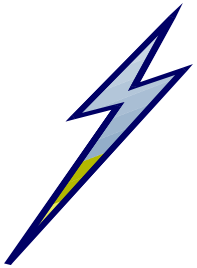
Threats Resulting in Crime or Loss

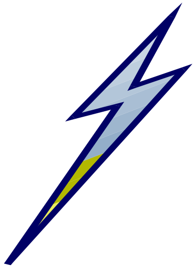


Source: *Computer Security Institute*

Natural Threats

- Fire
- Lightning
- Flood
- Earthquake





Unintentional Threats

- Accidents
- Carelessness
- Uninformed Actions
- Bad Habits

Intentional Threats

- Insiders
  - Computer Abuser
- Outsiders
  - Hacker
  - Corporate Raider
  - Foreign Intelligence

Intentional Insider - The "Computer Abuser"

Computer abuse is the intentional or unintentional misuse, abuse, destruction, alteration, or disruption of data processing resources.

- Access
- Motivation
- Safeguards

"The enemy is already in -- we hired them." Robert H. Courtney, Jr.

Vulnerability and threat analyses involves:

- IA analysis techniques are selected and used
- Vulnerabilities, their type, source, and severity are identified
- Threats, their type, source, and likelihood are identified
- Transaction paths, critical threat zones, and risk exposure are evaluated

IA Roadmap Steps

- Establish an IA organization
- Identify IA requirements
- Develop an acquisition IA strategy
- Secure resources for IA
- Initiate DITSCAP
- Incorporate IA solutions
- Test and evaluate IA solutions
- Accredit the system
- Maintain the system’s security posture throughout its life-cycle

http://www.eitoolkit.com/tools/initiation/info_assurance/02_ia_guide.doc

C&A Terminology

Certification: "Comprehensive evaluation of the **technical** and **non-technical** security features of an Automated Information System (AIS) and othe safeguards, made in support of the accreditation process to establish the extent to which a particular design and implementation meets a se of specified security requirements." *

* DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) 12/30/97

Accreditation: "Formal declaration by a Designated Approving Authority (DAA) that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk." *

* NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary January 1999.

C&A Guiding Policies

- DoDI 5200.40:
  - DoD Information Technology Security Certification and Accreditation Process (DITSCAP), Dec 1997.
- DoD 8510.1-M
  - DITSCAP Application Manual, July 31, 2000
  - Describes implementation activities and documentation
- DoDI 8500.1:
  - Information Assurance (IA), October 24, 2002
  - Supercedes older policies (DoD 5200.28, Orange Book)
- DoD 8500.2
  - Information Assurance (IA) Implementation, February 6, 2003
  - Establishes baseline IA Controls in accordance with Mission Assurance Categories

DoDD 8500.1

- IA requirements shall be included in all information system acquisitions or upgrades
- IA shall be “a visible element of all investment portfolios” including competitively-sourced IS
- All DoD IS shall be assigned an appropriate Mission Assurance Category
- Community risk shall be assessed and measures taken to mitigate that risk prior to interconnecting systems
- All DoD IS shall be certified and accredited IAW 5200.40
- All IA or IA-enabled IT must be validated in compliance with NSTISSP 11
- Systems enabling coalition operations shall be approved by the responsible Combatant Commander and DAAs

Baseline IA Levels – The Process

Determine the System Mission Assurance Category:

- Category I :
  - Vital to Effectiveness/Readiness of Deployed Forces
  - Any Loss Unacceptable
  - Immediate/Sustained Loss of Mission Effectiveness
  - Most Stringent Protection Measures Required
- Category II:
  - Important to Support Deployed Forces
  - Loss of Integrity Unacceptable; Loss of Availability Difficult to Manage
  - Loss/Degradation only tolerable for short term = May Seriously Impact Mission Effectiveness/Operational Readiness
  - Additional Safeguards Beyond Best Practices Required
- Category III:
  - Needed for Day-to-Day business, Does Not Affect Support to Deployed or Contingency Forces in the short-term
  - Loss Tolerated or Overcome without Significant Impact on Mission Effectiveness or Operational Readiness
  - Protective Measures Commensurate with Commercial Best Practices

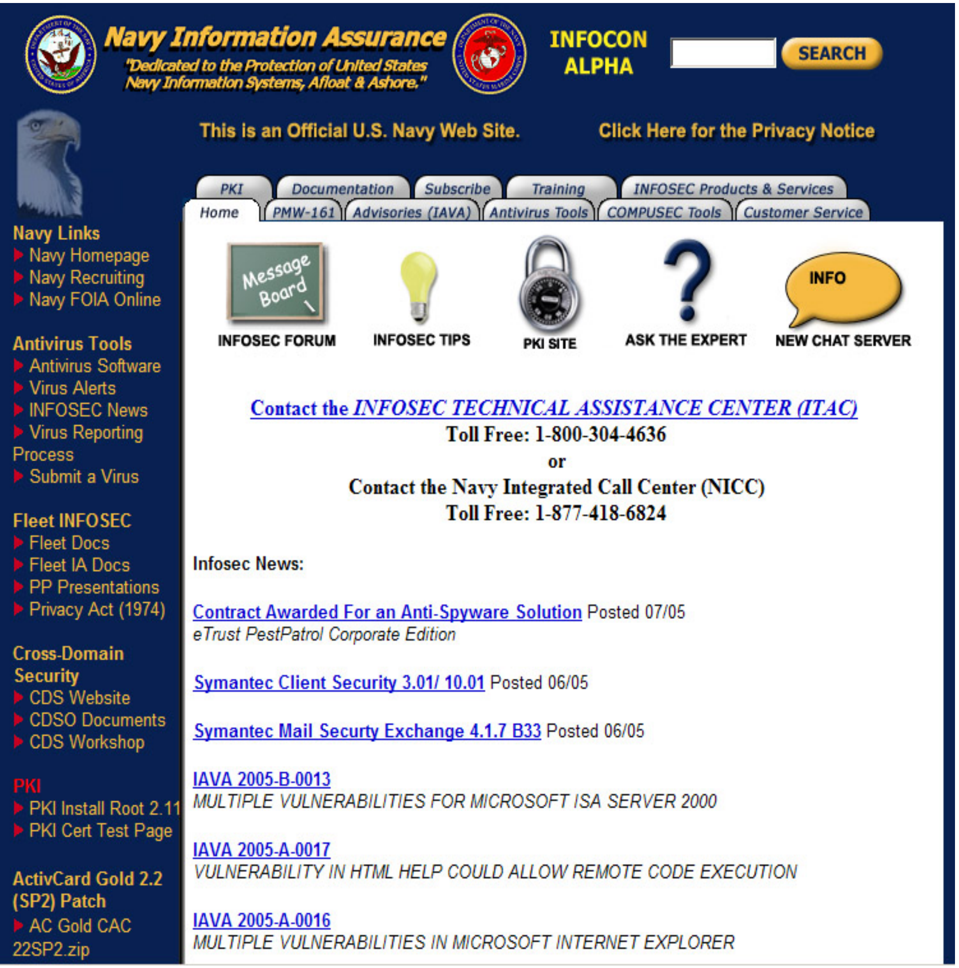
Example – DCSR -1 through -3 Security Design and Configuration

- MAC I -
  - *Only **high-robustness** GOTS or COTS IA and IA-enabled IT products are **used to protect classified information** when the information transits networks that are at a lower classification level than the information being transmitted.*
- MAC II –
  - *At a minimum, **medium-robustness** GOTS or COTS IA and IA-enabled IT products are **used to protect sensitive information** when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access information on the system**.***
- MAC III –
  - *At a minimum, **basic-robustnes**s GOTS or COTS IA and IA-enabled products are **used to protect publicly released information** from malicious tampering or destruction and ensure its availability.*

DoD IA Controls Subject Areas

- Security Design & Configuration
- Identification & Authentication
- Enclave & Computing Environment
- Enclave Boundary Defense
- Physical & Environmental
- Personnel
- Continuity
- Vulnerability & Incident Management

IA Web Resources



Navy Information Assurance

"Dedicated to the Protection of United States Navy Information Systems, Afloat & Ashore."

INFOCON ALPHA

SEARCH

This is an Official U.S. Navy Web Site.

Click Here for the Privacy Notice

Navy Links
- Navy Homepage
- Navy Recruiting
- Navy FOIA Online

Antivirus Tools
- Antivirus Software
- Virus Alerts
- INFOSEC News
- Virus Reporting Process
- Submit a Virus

Fleet INFOSEC
- Fleet Docs
- Fleet IA Docs
- PP Presentations
- Privacy Act (1974)

Cross-Domain Security
- CDS Website
- CDSO Documents
- CDS Workshop

PKI
- PKI Install Root 2.11
- PKI Cert Test Page

ActivCard Gold 2.2 (SP2) Patch
- AC Gold CAC 22SP2.zip

Contact the *INFOSEC TECHNICAL ASSISTANCE CENTER (ITAC)*
Toll Free: 1-800-304-4636
or
Contact the Navy Integrated Call Center (NICC)
Toll Free: 1-877-418-6824

Infosec News:

Contract Awarded For an Anti-Spyware Solution Posted 07/05
eTrust PestPatrol Corporate Edition

Symantec Client Security 3.01/ 10.01 Posted 06/05

Symantec Mail Securty Exchange 4.1.7 B33 Posted 06/05

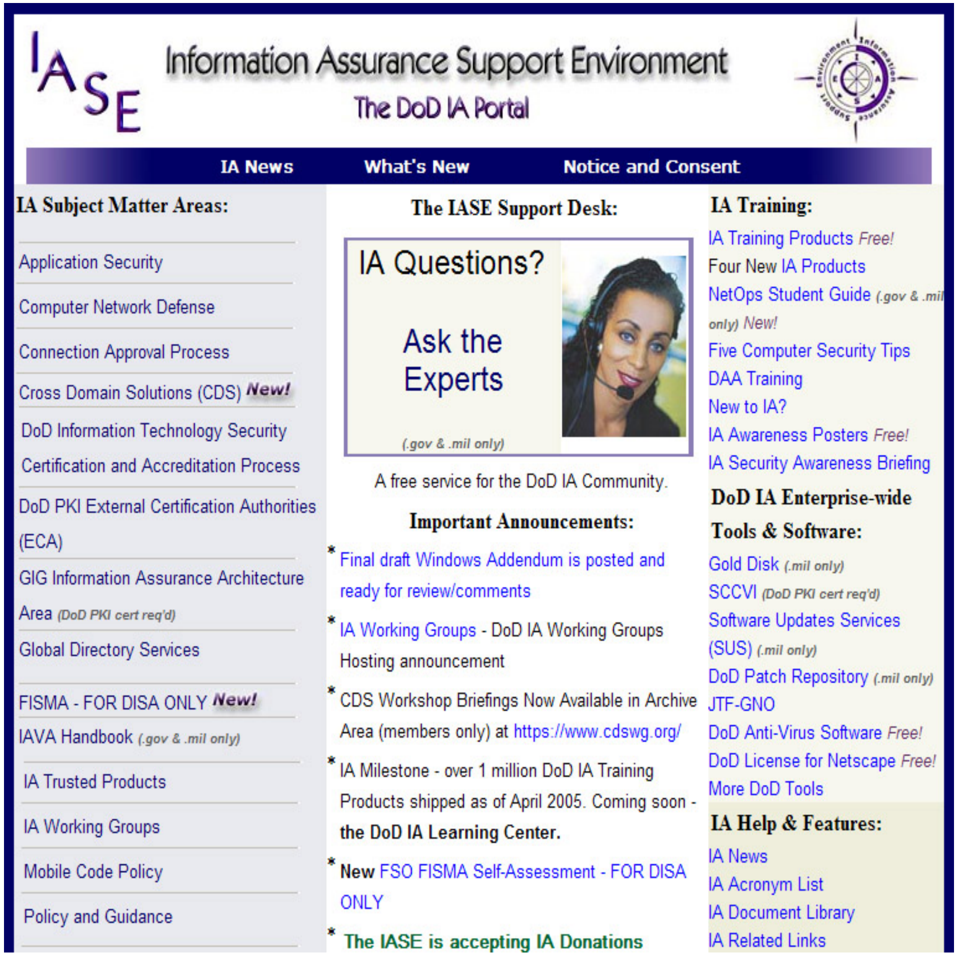
IAVA 2005-B-0013
MULTIPLE VULNERABILITIES FOR MICROSOFT ISA SERVER 2000

IAVA 2005-A-0017
VULNERABILITY IN HTML HELP COULD ALLOW REMOTE CODE EXECUTION

IAVA 2005-A-0016
MULTIPLE VULNERABILITIES IN MICROSOFT INTERNET EXPLORER

https://infosec.navy.mil/

https://infosec.navy.smil/



IASE Information Assurance Support Environment
The DoD IA Portal

IA News | What's New | Notice and Consent

IA Subject Matter Areas:

- Application Security
- Computer Network Defense
- Connection Approval Process
- Cross Domain Solutions (CDS) *New!*
- DoD Information Technology Security Certification and Accreditation Process
- DoD PKI External Certification Authorities (ECA)
- GIG Information Assurance Architecture Area *(DoD PKI cert req'd)*
- Global Directory Services
- FISMA - FOR DISA ONLY *New!*
- IAVA Handbook *(.gov & .mil only)*
- IA Trusted Products
- IA Working Groups
- Mobile Code Policy
- Policy and Guidance

The IASE Support Desk:

IA Questions?

Ask the Experts

(.gov & .mil only)

A free service for the DoD IA Community.

Important Announcements:

* Final draft Windows Addendum is posted and ready for review/comments
* IA Working Groups - DoD IA Working Groups Hosting announcement
* CDS Workshop Briefings Now Available in Archive Area (members only) at https://www.cdswg.org/
* IA Milestone - over 1 million DoD IA Training Products shipped as of April 2005. Coming soon - **the DoD IA Learning Center.**
* **New** FSO FISMA Self-Assessment - FOR DISA ONLY
* **The IASE is accepting IA Donations**

IA Training:

IA Training Products *Free!*
Four New IA Products
NetOps Student Guide *(.gov & .mil only)* *New!*
Five Computer Security Tips
DAA Training
New to IA?
IA Awareness Posters *Free!*
IA Security Awareness Briefing

DoD IA Enterprise-wide Tools & Software:

Gold Disk *(.mil only)*
SCCVI *(DoD PKI cert req'd)*
Software Updates Services (SUS) *(.mil only)*
DoD Patch Repository *(.mil only)*
JTF-GNO
DoD Anti-Virus Software *Free!*
DoD License for Netscape *Free!*
More DoD Tools

IA Help & Features:

IA News
IA Acronym List
IA Document Library
IA Related Links

http://iase.disa.mil/policy.html#Acquisition